

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-243

Vulnerability Summary for the Week of August 24, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
2enetworkx -- openforum	OpenForum 0.66 Beta allows remote attackers to bypass authentication and reset passwords of other users via a direct request with the update parameter set to 1 and modified user and password parameters.	2009-08-25	7.5	CVE-2008-7066 XF BID MILWORM	
adium -- adium pidgin -- pidgin	The msn_slplink_process_msg function in libpurple/protocols/msn/slplink.c in libpurple, as used in Pidgin (formerly Gaim) before 2.5.9 and Adium 1.3.5 and earlier, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) by sending multiple crafted SLP (aka MSNSLP) messages to trigger an overwrite of an arbitrary memory location. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2009-1376.	2009-08-21	10.0	CVE-2009-2694 DEBIAN CONFIRM	
aled_owen -- one-news	SQL injection vulnerability in index.php in One-News Beta 2 allows remote attackers to execute arbitrary SQL commands via the q parameter.	2009-08-24	7.5	CVE-2008-7059 XF BID BUGTRAQ	
arubanetworks -- aruba_mobility_controller arubanetworks -- arubaos	Aruba Mobility Controller running ArubaOS 3.3.1.16, and possibly other versions, installs the same default X.509 certificate for all installations, which allows remote attackers to bypass authentication. NOTE: this is only a vulnerability when the administrator does not follow recommendations in the product's security documentation.	2009-08-21	10.0	CVE-2008-7023 BID BUGTRAQ BUGTRAQ OSVDB	
	The SNMP daemon in ArubaOS 3.3.2.6 in Aruba Mobility Controller does not restrict SNMP access,				

arubanetworks -- arubaos	which allows remote attackers to (1) read all SNMP community strings via SNMP-COMMUNITY-MIB::snmpCommunityName (1.3.6.1.6.3.18.1.1.1.2) or SNMP-VIEW-BASED-ACM-MIB::vacmGroupName (1.3.6.1.6.3.16.1.2.1.3) with knowledge of one community string, and (2) read SNMPv3 user names via SNMP-USER-BASED-SM-MIB or SNMP-VIEW-BASED-ACM-MIB.	2009-08-27	7.8	CVE-2008-7095 BID BUGTRAQ OSVDB
aves -- rpg_board	RPG.Board 0.8 Beta2 and earlier allows remote attackers to bypass authentication and gain privileges by setting the keep4u cookie to a certain value.	2009-08-21	7.5	CVE-2008-7028 XF BID MILWORM
belkin -- f5d7632-4 belkin -- wireless_g_router	The web interface to the Belkin Wireless G router and ADSL2 modem F5D7632-4V6 with firmware 6.01.08 allows remote attackers to bypass authentication and gain administrator privileges via a direct request to (1) statusprocess.exe, (2) system_all.exe, or (3) restore.exe in cgi-bin/. NOTE: the setup_dns.exe vector is already covered by CVE-2008-1244.	2009-08-28	10.0	CVE-2008-7115 XF SECTRACK MILWORM SECUNIA
chipmunk-scripts -- chipmunk_topsites	SQL injection vulnerability in authenticate.php in Chipmunk Topsites allows remote attackers to execute arbitrary SQL commands via the username parameter, related to login.php. NOTE: some of these details are obtained from third party information.	2009-08-25	7.5	CVE-2008-7071 XF BID MILWORM
cisco -- firewall_services_module	The Cisco Firewall Services Module (FWSM) 2.x, 3.1 before 3.1(16), 3.2 before 3.2(13), and 4.0 before 4.0(6) for Cisco Catalyst 6500 switches and Cisco 7600 routers allows remote attackers to cause a denial of service (traffic-handling outage) via a series of malformed ICMP messages.	2009-08-21	7.8	CVE-2009-0638 BID CISCO
cisco -- unified_communications_manager	Cisco Unified Communications Manager (aka CUCM, formerly CallManager) before 6.1(1) allows remote attackers to cause a denial of service (voice-services outage) via a malformed header in a SIP message, aka Bug ID CSCsi46466.	2009-08-27	7.8	CVE-2009-2050 CISCO
cisco -- unified_communications_manager	Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), and 7.x before 7.1(2) allows remote attackers to cause a denial of service (voice-services outage) via a malformed SIP INVITE message that triggers an improper call to the sipSafeStrlen function, aka Bug ID CSCsz40392.	2009-08-27	7.8	CVE-2009-2051 CISCO
cisco -- unified_communications_manager	Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), 7.0 before 7.0(2), and 7.1 before 7.1(2) allows remote attackers to cause a denial of service (TCP services outage) via a large number of TCP connections, related to "tracking of network connections," aka Bug ID CSCsq22534.	2009-08-27	7.8	CVE-2009-2052 CISCO
cisco -- unified_communications_manager	Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), 7.0 before 7.0(2a)su1, and 7.1 before 7.1(2) allows remote attackers to cause a denial of service (file-descriptor exhaustion and SCCP outage) via a flood of TCP packets, aka Bug ID CSCsx32236.	2009-08-27	7.8	CVE-2009-2053 CISCO
cisco -- unified_communications_manager	Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.x, 5.x before 5.1(3g), 6.x before 6.1(4), 7.0 before 7.0(2a)su1, and 7.1 before 7.1(2a)su1 allows remote attackers to cause a denial of service (file-descriptor exhaustion and SIP outage) via a flood of TCP packets, aka Bug ID CSCsx23689.	2009-08-27	7.8	CVE-2009-2054 CISCO
	The Over-the-Air Provisioning (OTAP) functionality			

cisco -- aironet_ap1100 cisco -- aironet_ap1200	on Cisco Aironet Lightweight Access Point 1100 and 1200 devices does not properly implement access-point association, which allows remote attackers to spoof a controller and cause a denial of service (service outage) via crafted remote radio management (RRM) packets, aka "SkyJack" or Bug ID CSCtb56664.	2009-08-27	7.3	CVE-2009-2861 CONFIRM
cisco -- aironet_ap1100 cisco -- aironet_ap1200	Cisco Aironet Lightweight Access Point (AP) devices send the contents of certain multicast data frames in cleartext, which allows remote attackers to discover Wireless LAN Controller MAC addresses and IP addresses, and AP configuration details, by sniffing the wireless network.	2009-08-27	7.8	CVE-2009-2976 MISC MISC SECTRACK
cuteflow -- cuteflow	CuteFlow 2.10.3 and 2.11.0_c does not properly restrict access to pages/edituser.php, which allows remote attackers to modify usernames and passwords via a direct request.	2009-08-25	7.5	CVE-2009-2960 BID BUGTRAQ SECUNIA
decomputeur -- toolbar_uninstaller	Unspecified vulnerability in the update feature in Toolbar Uninstaller 1.0.2 allows remote attackers to force the download and execution of arbitrary files via attack vectors related to a "malformed update url and a malformed update website."	2009-08-25	9.3	CVE-2009-2963 XF CONFIRM SECUNIA
dotnetnuke -- dotnetnuke	DotNetNuke 2.0 through 4.8.4 allows remote attackers to load .ascx files instead of skin files, and possibly access privileged functionality, via unknown vectors related to parameter validation.	2009-08-27	7.5	CVE-2008-7102 CONFIRM
eset -- smart_security	easdrv.sys in ESET Smart Security 3.0.667.0 allows local users to cause a denial of service (crash) via a crafted IOCTL 0x222003 request to the \\.\easdrv device interface.	2009-08-28	7.2	CVE-2008-7107 XF BID MILWORM
esqlanelapse -- esqlanelapse	Esqlanelapse 2.6.1 and 2.6.2 allows remote attackers to bypass authentication and gain privileges via modified (1) enombre and (2) euri cookies.	2009-08-21	7.5	CVE-2008-7019 XF BID MILWORM
google -- chrome	Google V8, as used in Google Chrome before 2.0.172.43, allows remote attackers to bypass intended restrictions on reading memory, and possibly obtain sensitive information or execute arbitrary code in the Chrome sandbox, via crafted JavaScript.	2009-08-27	10.0	CVE-2009-2935 VUPEN BID SECUNIA CONFIRM CONFIRM
ifusionservices -- ifdate	SQL injection vulnerability in members_search.php in iFusion Services ifDate 2.0.3 and earlier allows remote attackers to execute arbitrary SQL commands via the name field.	2009-08-28	7.5	CVE-2008-7114 XF BID MILWORM
itn -- itn_news_gadget	The Sidebar gadget in ITN News Gadget (aka ITN Hub Gadget) 1.06 for Windows Vista, and possibly other versions before 1.23, allows remote web servers or man-in-the-middle attackers to execute arbitrary commands via script in a short_title response.	2009-08-24	7.5	CVE-2008-7037 XF BID MISC
kalptaru_infotech -- stararticles	Multiple SQL injection vulnerabilities in Kalptaru Infotech Ltd. Star Articles 6.0 allow remote attackers to inject arbitrary SQL commands via (1) the subcatid parameter to article.list.php; or the artid parameter to (2) article.print.php, (3) article.comments.php, (4) article.publisher.php, or (5) article.download.php; and (6) the PATH_INFO to article.download.php. NOTE: some of these details are obtained from third party	2009-08-25	7.5	CVE-2008-7075 XF VUPEN BID MILWORM MILWORM SECUNIA OSVDB OSVDB

	information.			OSVDB OSVDB OSVDB
kolmck -- kol_player	Stack-based buffer overflow in Thaddy de Konng KOL Player 1.0 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL in a .MP3 playlist file.	2009-08-25	9.3	CVE-2009-2961 XF MILWORM
kvirc -- kvirc	Argument injection vulnerability in the URI handler in KVirc 3.4.2 Shiny allows remote attackers to execute arbitrary commands via a " (quote) followed by command line switches in a (1) irc:/// , (2) irc6:/// , (3) ircs:/// , or (4) and ircs6:/// URI. NOTE: this might be due to an incomplete fix for CVE-2007-2951.	2009-08-25	9.3	CVE-2008-7070 XF BID BUGTRAQ MILWORM MISC
kyocera -- kyocera_mita	Directory traversal vulnerability in the Scanner File Utility (aka listener) in Kyocera Mita (KM) 3.3.0.1 allows remote attackers to upload files to arbitrary locations via a .. (dot dot) in a request.	2009-08-28	7.8	CVE-2008-7110 XF BID BUGTRAQ MISC SECUNIA
kyoceramita -- scanner_file_utility	The Scanner File Utility (aka listener) in Kyocera Mita (KM) 3.3.0.1 allows remote attackers to bypass authorization and upload arbitrary files to the client system via a modified program that does not prompt the user for a password.	2009-08-28	10.0	CVE-2008-7109 XF BID BUGTRAQ MISC SECUNIA
kyoceramita -- scanner_file_utility	The Scanner File Utility (aka listener) in Kyocera Mita (KM) 3.3.0.1 does not restrict the filenames or extensions of uploaded files, which makes it easier for remote attackers to execute arbitrary code or overwrite files by leveraging CVE-2008-7110 and CVE-2008-7109.	2009-08-28	9.3	CVE-2008-7111 BUGTRAQ MISC SECUNIA
linux -- kernel	The UDP implementation in (1) net/ipv4/udp.c and (2) net/ipv6/udp.c in the Linux kernel before 2.6.19 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving the MSG_MORE flag and a UDP socket.	2009-08-27	7.2	CVE-2009-2698 CONFIRM CONFIRM SECUNIA SECUNIA REDHAT REDHAT CONFIRM
logmein -- racctrl.dll	LogMeIn Remote Access Utility ActiveX control (RACctrl.dll) allows remote attackers to cause a denial of service (crash) by setting the fgcolor and bgcolor properties to certain long values that trigger memory corruption.	2009-08-24	9.3	CVE-2008-7053 XF BID MILWORM MISC
maiascriptworld -- maian_greetings	Maian Greetings 2.1 allows remote attackers to bypass authentication and gain administrative privileges by setting the mecard_admin_cookie cookie to admin.	2009-08-26	7.5	CVE-2008-7086 XF BID MILWORM
maxum -- rumpus	Multiple buffer overflows in Rumpus before 6.0.1 allow remote attackers to (1) cause a denial of service (segmentation fault) via a long HTTP verb in the HTTP component; and allow remote authenticated users to execute arbitrary code via a long argument to the (2) MKD, (3) XMKD, (4) RMD, and other unspecified commands in the FTP component.	2009-08-25	9.0	CVE-2008-7078 XF XF BID BID BUGTRAQ MILWORM CONFIRM

				SECUNIA FULLDISC
memcode -- i.scribe	Format string vulnerability in MemeCode Software i.Scribe 1.88 through 2.00 before Beta9 allows remote SMTP servers to cause a denial of service (crash) and possibly execute arbitrary code via format string specifiers in a server response, which is not properly handled "when displaying the signon message."	2009-08-25	9.3	CVE-2008-7074 XF BID MILWORM SECUNIA OSVDB CONFIRM
mregiguy -- hot_links_sql-php	SQL injection vulnerability in Mr. CGI Guy Hot Links SQL-PHP 3 and earlier allows remote attackers to execute arbitrary SQL commands via the news.php parameter.	2009-08-28	7.5	CVE-2008-7120 BID MISC
najdi.si -- toolbar	Stack-based buffer overflow in an ActiveX control in najdisitoolbar.dll in Najdi.si Toolbar 2.0.4.1 allows remote attackers to cause a denial of service (browser crash) or execute arbitrary code via a long Document.Location property value.	2009-08-27	9.3	CVE-2008-7103 XF BID MILWORM SECUNIA OSVDB
nero -- showtime	Buffer overflow in Nero ShowTime 5.0.15.0 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long entry in a .M3U playlist file. NOTE: this issue might be related to CVE-2008-0619.	2009-08-25	9.3	CVE-2008-7079 XF BID MILWORM SECUNIA OSVDB
openpro -- openpro	PHP remote file inclusion vulnerability in search_wA.php in OpenPro 1.3.1 allows remote attackers to execute arbitrary PHP code via a URL in the LIBPATH parameter.	2009-08-26	7.5	CVE-2008-7087 BID BUGTRAQ OSVDB
pagetreecms -- page_tree_cms	PHP remote file inclusion vulnerability in admin/plugins/Online_Users/main.php in PageTree CMS 0.0.2 BETA 0001 allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[PT_Config][dir][data] parameter.	2009-08-25	7.5	CVE-2008-7067 XF BID MILWORM
paul_arbogast -- accms	All Club CMS (ACCMS) 0.0.2 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain database configuration information, including credentials, via a direct request to accms.dat.	2009-08-25	7.5	CVE-2008-7069 XF MILWORM
pligg -- pligg_cms	Multiple directory traversal vulnerabilities in Pligg 9.9 and earlier allow remote attackers to (1) determine the existence of arbitrary files via a .. (dot dot) in the \$tb_url variable in trackback.php, or (2) include arbitrary files via a .. (dot dot) in the template parameter to settemplate.php.	2009-08-26	7.8	CVE-2008-7090 XF XF BID BUGTRAQ OSVDB OSVDB MILWORM MISC
pligg -- pligg_cms	Multiple SQL injection vulnerabilities in Pligg 9.9 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to vote.php, which is not properly handled in libs/link.php; (2) id parameter to trackback.php; (3) an unspecified parameter to submit.php; (4) requestTitle variable in a query to story.php; (5) requestID and (6) requestTitle variables in recommend.php; (7) categoryID	2009-08-26	7.5	CVE-2008-7091 XF BID BUGTRAQ OSVDB OSVDB OSVDB OSVDB OSVDB

	<p>variables in recommend.php, (7) category parameter to cloud.php; (8) title parameter to out.php; (9) username parameter to login.php; (10) id parameter to cvote.php; and (11) commentid parameter to edit.php.</p>			OSVDB OSVDB OSVDB OSVDB OSVDB MILWORM MISC
qsoft -- k-rate	Multiple SQL injection vulnerabilities in Qsoft K-Rate Premium allow remote attackers to execute arbitrary SQL commands via (1) the \$id variable in admin/includes/dele_cpac.php, (2) \$ord[order_id] variable in payments/payment_received.php, (3) \$id variable in includes/functions.php, and (4) unspecified variables in modules/chat.php, as demonstrated via the (a) show parameter in an online action to index.php; (b) PATH_INTO to the room/ handler; (c) image and (d) id parameters in a vote action to index.php; (e) PATH_INFO to the blog/ handler; and (f) id parameter in a blog_edit action to index.php.	2009-08-27	7.5	CVE-2008-7097 XF MILWORM SECUNIA OSVDB
qsoft -- k-rate	Unspecified vulnerability in the Manage Templates feature in Qsoft K-Rate Premium allows remote attackers to execute arbitrary PHP code via unknown vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-27	7.5	CVE-2008-7099 MILWORM SECUNIA OSVDB
quicksilver_forums -- quicksilver_forums	Directory traversal vulnerability in the get_lang function in global.php in Quicksilver Forums 1.4.2 and earlier, when running on Windows, allows remote attackers to include and execute arbitrary local files via a "\\" (backslash) in the lang parameter to index.php, which bypasses a protection mechanism that only checks for "/" (forward slash), as demonstrated by uploading and including PHP code in an avatar file.	2009-08-25	7.5	CVE-2008-7064 XF XF BID MILWORM SECUNIA OSVDB
raidsionic -- icy_box_nas	userHandler.cgi in RaidSonic ICY BOX NAS firmware 2.3.2.IB.2.RS.1 allows remote attackers to bypass authentication and gain administrator privileges by setting the login parameter to admin. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-25	10.0	CVE-2008-7081 XF BID
relative -- sailplanner	Multiple SQL injection vulnerabilities in SailPlanner 0.3a allow remote attackers to execute arbitrary SQL commands via the (1) username and (2) password fields.	2009-08-25	7.5	CVE-2008-7077 XF BID MILWORM MISC
revou -- micro_blogging_twitter_clone	Multiple SQL injection vulnerabilities in ReVou Micro Blogging Twitter clone allow remote attackers to execute arbitrary SQL commands via the (1) username and (2) password fields.	2009-08-25	7.5	CVE-2008-7083 XF BID MILWORM
siemens -- gigaset_c450_ip siemens -- gigaset_c475_ip	Siemens C450 IP and C475 IP VoIP devices allow remote attackers to cause a denial of service (disconnected calls and device reboot) via a crafted SIP packet to UDP port 5060.	2009-08-25	7.8	CVE-2008-7065 XF BID BUGTRAQ MILWORM SECUNIA OSVDB
site2nite -- real_estate_web	Multiple SQL injection vulnerabilities in Site2Nite Real Estate Web allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password field to an unspecified component, possibly	2009-08-24	7.5	CVE-2008-7030 XF BID

	agentlist.asp. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect.			BUGTRAQ OSVDB
slideshowpro -- director	Directory traversal vulnerability in p.php in SlideShowPro Director 1.1 through 1.3.8 allows remote attackers to read arbitrary files via directory traversal sequences in the a parameter.	2009-08-21	7.8	CVE-2009-2931 BUGTRAQ OSVDB MISC CONFIRM SECUNIA
sugarcrm -- sugarcrm	SQL injection vulnerability in SugarCRM 4.5.10 and earlier, 5.0.0k and earlier, and 5.2.0g and earlier, allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-08-27	7.5	CVE-2009-2978 CONFIRM CONFIRM JVN
sun -- solaris	in.lpd in the print service in Sun Solaris 8 and 9 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors that trigger a "fork()/exec() bomb."	2009-08-27	7.8	CVE-2009-2972 VUPEN BID SUNALERT CONFIRM
thehockeystop -- hockeystats_online	Multiple SQL injection vulnerabilities in TheHockeyStop HockeySTATS Online 2.0 Basic and Advanced allow remote attackers to execute arbitrary SQL commands via the (1) id parameter in the viewpage action to the default URI, probably index.php, or (2) divid parameter in the schedule action to index.php.	2009-08-26	7.5	CVE-2008-7085 XF BID MILWORM
tigran_abrahamyan -- phpecho_cms	PHP remote file inclusion vulnerability in kernel/smarty/Smarty.class.php in PHPEcho CMS 2.0 rc3 allows remote attackers to execute arbitrary PHP code via a URL in unspecified vectors that modify the _smarty_compile_path variable in the fetch function.	2009-08-24	7.5	CVE-2008-7034 XF BID OSVDB BUGTRAQ
tikiwiki -- tikiwiki	TikiWiki 1.6.1 allows remote attackers to bypass authentication by entering a valid username with an arbitrary password, possibly related to the Internet Explorer "Remember Me" feature. NOTE: some of these details are obtained from third party information.	2009-08-24	7.5	CVE-2003-1574 BID CONFIRM
webidsupport -- webid	SQL injection vulnerability in the admin panel (admin/) in WeBid auction script 0.5.4 allows remote attackers to execute arbitrary SQL commands via the username.	2009-08-28	7.5	CVE-2008-7116 XF BID MILWORM
webidsupport -- webid	SQL injection vulnerability in item.php in WeBid auction script 0.5.4 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-08-28	7.5	CVE-2008-7119 XF BID MILWORM

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bitmixsoft -- php-lance	Multiple directory traversal vulnerabilities in BitmixSoft PHP-Lance 1.52 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) language parameter to show.php and (2) in parameter to advanced_search.php.	2009-08-21	5.0	CVE-2009-2923 MILWORM OSVDB OSVDB
	Cross-site scripting (XSS) vulnerability in the waterfall web status view			CVE-2009-2959 FEDORA

buildbot -- buildbot	(status/web/waterfall.py) in Buildbot 0.7.6 through 0.7.11p1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-08-25	4.3	FEDORA VUPEN BID MLIST CONFIRM
buildbot -- buildbot	Multiple cross-site scripting (XSS) vulnerabilities in Buildbot 0.7.6 through 0.7.11p2 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, different vulnerabilities than CVE-2009-2959.	2009-08-26	4.3	CVE-2009-2967 VUPEN CONFIRM
carmosa -- phpcart	Multiple cross-site scripting (XSS) vulnerabilities in Carmosa phpCart 3.4 through 4.6.4 allow remote attackers to inject arbitrary web script or HTML via the (1) quantity or (2) Add Engraving fields to the default URI; (3) Quantity field to phpcart.php; (4) Name, (5) Company, (6) Address, (7) City, and (8) Province/State fields in a checkout action to phpcart.php; and other unspecified vectors.	2009-08-28	4.3	CVE-2008-7108 XF BID BUGTRAQ
chipmunk-scripts -- chipmunk_topsites	Cross-site scripting (XSS) vulnerability in index.php in Chipmunk Topsites allows remote attackers to inject arbitrary web script or HTML via the start parameter.	2009-08-25	4.3	CVE-2008-7072 XF BID MILWoRM
dotnetnuke -- dotnetnuke	Unspecified vulnerability in DotNetNuke 4.4.1 through 4.8.4 allows remote authenticated users to bypass authentication and gain privileges via unknown vectors related to a "unique id" for user actions and improper validation of a "user identity."	2009-08-27	6.5	CVE-2008-7100 BID CONFIRM
dotnetnuke -- dotnetnuke	Unspecified vulnerability in DotNetNuke 4.0 through 4.8.4 and 5.0 allows remote attackers to obtain sensitive information (portal number) by accessing the install wizard page via unknown vectors.	2009-08-27	5.0	CVE-2008-7101 CONFIRM
ekkaia -- pie_web rssmodule -- rss_module	PHP remote file inclusion vulnerability in lib/action/rss.php in RSS module 0.1 for Pie Web M{a,e}sher, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the lib parameter.	2009-08-25	6.8	CVE-2008-7073 XF MISC BID MILWoRM
elvinbts -- elvinbts	Multiple cross-site scripting (XSS) vulnerabilities in Elvin 1.2.2 allow remote attackers to inject arbitrary web script or HTML via the (1) component and (2) priority parameters to buglist.php; and the (3) Username (4) E-mail, (5) Pass, and (6) Confirm pass fields to createaccount.php.	2009-08-21	4.3	CVE-2009-2920 XF MILWoRM
f5 -- big-ip	Web Management Console Cross-site request forgery (CSRF) vulnerability in the web management console in F5 BIG-IP 9.4.3 allows remote attackers to hijack the authentication of administrators for requests that create new administrators and execute shell commands, as demonstrated using tmui/Control/form.	2009-08-24	6.8	CVE-2008-7032 XF BID BUGTRAQ BUGTRAQ OSVDB
google -- chrome	The tooltip manager (chrome/views/tooltip_manager.cc) in Google Chrome 0.2.149.29 Build 1798 and possibly other versions before 0.2.149.30 allows remote attackers to cause a denial of service (CPU consumption or crash) via a tag with a long title attribute, which is not properly handled	2009-08-24	4.3	CVE-2008-7061 MISC MTS

	when displaying a tooltip, a different vulnerability than CVE-2008-6994. NOTE: there is inconsistent information about the environments under which this issue exists.			MISC
google -- chrome	Google Chrome before 2.0.172.43 does not prevent SSL connections to a site with an X.509 certificate signed with the (1) MD2 or (2) MD4 algorithm, which makes it easier for man-in-the-middle attackers to spoof arbitrary HTTPS servers via a crafted certificate, a related issue to CVE-2009-2409.	2009-08-27	6.4	CVE-2009-2973 VUPEN SECUNIA CONFIRM CONFIRM
google -- chrome	Google Chrome 1.0.154.65, 1.0.154.48, and earlier allows remote attackers to (1) cause a denial of service (application hang) via vectors involving a chromehtml: URI value for the document.location property or (2) cause a denial of service (application hang and CPU consumption) via vectors involving a series of function calls that set a chromehtml: URI value for the document.location property.	2009-08-27	5.0	CVE-2009-2974 MISC BUGTRAQ BUGTRAQ
grayscalecms -- bandsite_cms	BandSite CMS 1.1.4 does not perform access control for adminpanel/phpmydump.php, which allows remote attackers to obtain copies of the database via a direct request.	2009-08-24	5.0	CVE-2008-7056 XF BID MILWoRM SECUNIA
grayscalecms -- bandsite_cms	Cross-site scripting (XSS) vulnerability in merchandise.php in BandSite CMS 1.1.4 allows remote attackers to inject arbitrary HTML or web script via the type parameter.	2009-08-24	4.3	CVE-2008-7057 XF BID MILWoRM SECUNIA
grayscalecms -- bandsite_cms	Cross-site request forgery (CSRF) vulnerability in BandSite CMS 1.1.4 allows remote attackers to hijack the authentication of administrators and force a logout via adminpanel/logout.php.	2009-08-24	6.8	CVE-2008-7058 XF BID MILWoRM
hirschelectronics -- velocity_security_management_system	Directory traversal vulnerability in the web server 1.0 in Velocity Security Management System allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.	2009-08-26	5.0	CVE-2008-7084 XF BID BUGTRAQ MILWoRM OSVDB
ibm -- websphere_commerce_suite	The (1) Net.Commerce and (2) Net.Data components in IBM WebSphere Commerce Suite store sensitive information under the web root with insufficient access control, which allows remote attackers to discover passwords, and database and filesystem details, via direct requests for configuration files.	2009-08-24	5.0	CVE-2009-2956 XF
intel -- bios	Intel Desktop and Intel Mobile Boards with BIOS firmware DQ35JO, DQ35MP, DP35DP, DG33FB, DG33BU, DG33TL, MGM965TW, D945GCPE, and DX38BT allows local administrators with ring 0 privileges to gain additional privileges and modify code that is running in System Management Mode, or access hypervisor memory as demonstrated at Black Hat 2008 by accessing certain remapping registers in Xen 3.3.	2009-08-27	6.8	CVE-2008-7096 CONFIRM
	K-Meleon 1.5.3 allows context-dependent attackers to spoof the address bar, via			CVE-2009-2960

k-meleon_project -- k-meleon	window.open with a relative URI, to show an arbitrary file: URL after a victim has visited any file: URL, as demonstrated by a visit to a file: document written by the attacker.	2009-08-28	5.8	CVE-2009-3008 MISC
kalptaru_infotech -- stararticles	Unrestricted file upload vulnerability in user.modify.profile.php in Kalptaru Infotech Ltd. Star Articles 6.0 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a profile photo, then accessing it via a direct request to the file in authorphoto/.	2009-08-25	6.5	CVE-2008-7076 XF BID MILWoRM SECUNIA OSVDB
kaspersky -- kaspersky_anti-virus kaspersky -- kaspersky_internet_security	avp.exe in Kaspersky Internet Security 9.0.0.459 and Anti-Virus 9.0.0.463 allows remote attackers to cause a denial of service (CPU consumption and network connectivity loss) via an HTTP URL request that contains a large number of dot "." characters.	2009-08-25	4.3	CVE-2009-2966 XF SECTRACK SECTRACK BID OSVDB MISC SREASONRES SECUNIA FULLDISC
kyoceramita -- scanner_file_utility	The Scanner File Utility (aka listener) in Kyocera Mita (KM) 3.3.0.1 allows remote attackers to cause a denial of service (hang or crash) via invalid field length values in a malformed (1) document or (2) request.	2009-08-28	5.0	CVE-2008-7112 XF MISC SECUNIA
kyoceramita -- scanner_file_utility	The Scanner File Utility (aka listener) in Kyocera Mita (KM) 3.3.0.1 uses a small space of predictable user identification numbers for access control, which allows remote attackers to upload documents via a brute force attack.	2009-08-28	6.4	CVE-2008-7113 XF MISC SECUNIA
lovecms -- lovecms	Unrestricted file upload vulnerability in admin/index.php in Download Manager module 1.0 for LoveCMS 1.6.2 Final allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in uploads/.	2009-08-25	6.8	CVE-2008-7062 XF MILWoRM SECUNIA OSVDB
mozilla -- firefox	Mozilla Firefox 3.0.6 through 3.0.13, and 3.5.x, allows remote attackers to cause a denial of service (CPU consumption) via JavaScript code with a long string value for the hash property (aka location.hash), a related issue to CVE-2008-5715.	2009-08-24	5.0	CVE-2009-2953 BUGTRAQ MISC
mozilla -- firefox	Mozilla Firefox 3.5.2 on Windows XP, in some situations possibly involving an incompletely configured protocol handler, does not properly implement setting the document.location property to a value specifying a protocol associated with an external application, which allows remote attackers to cause a denial of service (memory consumption) via vectors involving a series of function calls that set this property, as demonstrated by (1) the chromehtml: protocol and (2) the aim: protocol.	2009-08-27	5.0	CVE-2009-2975 BUGTRAQ BUGTRAQ BUGTRAQ
mrcgiguy -- hot_links_sql-php	Cross-site scripting (XSS) vulnerability in Mr. CGI Guy Hot Links SQL-PHP 3 and earlier allows remote attackers to inject arbitrary web script or HTML via the search bar.	2009-08-28	4.3	CVE-2008-7121 MISC
	MyBB (aka MyBulletinBoard) 1.4.3 includes the sensitive my_post_key parameter in URLs to			CVE-2008-

mybboard -- mybb	moderation.php with the (1) mergeposts, (2) split, and (3) deleteposts actions, which allows remote attackers to steal the token and bypass the cross-site request forgery (CSRF) protection mechanism to hijack the authentication of moderators by reading the token from the HTTP Referer header.	2009-08-25	6.8	7082 XF BID BUGTRAQ SECUNIA OSVDB
ocean12tech -- faq_manager_pro	Ocean12 FAQ Manager Pro stores sensitive data under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for admin/o12faq.mdb.	2009-08-25	5.0	CVE-2008-7063 XF MILWoRM
one-news -- one-news	Multiple cross-site scripting (XSS) vulnerabilities in One-News Beta 2 allow remote attackers to inject arbitrary HTML and web script via the (1) title or (2) content parameters in a news item to add.php, and the (3) itemnum, (4) author, or (5) comment parameters in a comment to index.php. NOTE: vectors 1 and 2 require user authentication.	2009-08-24	4.3	CVE-2008-7060 XF XF BID BUGTRAQ
photopost -- photopost_vbgallery	Unrestricted file upload vulnerability in upload.php in PhotoPost vBGallery 2.4.2 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension followed by a safe extension, then accessing it via a direct request to the file in a certain path. NOTE: this may be the same vulnerability as CVE-2008-0251, but this is not clear due to lack of details from the vendor.	2009-08-26	6.5	CVE-2008-7088 XF BID MILWoRM
php -- php	The dba_replace function in PHP 5.2.6 and 4.x allows context-dependent attackers to cause a denial of service (file truncation) via a key with the NULL byte. NOTE: this might only be a vulnerability in limited circumstances in which the attacker can modify or add database entries but does not have permissions to truncate the file.	2009-08-25	6.4	CVE-2008-7068 XF BUGTRAQ BUGTRAQ BUGTRAQ OSVDB SREASONRES CONFIRM
phpclassifiedsscript -- php_classifieds_script	Team PHP PHP Classifieds Script stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain database credentials via a direct request for admin/backup/datadump.sql.	2009-08-25	5.0	CVE-2008-7080 XF OSVDB MILWoRM SECUNIA
pligg -- pligg_cms	Cross-site scripting (XSS) vulnerability in Pligg 9.9 and earlier allows remote attackers to inject arbitrary web script or HTML via the keyword parameter in a search action to user.php and other unspecified vectors.	2009-08-26	4.3	CVE-2008-7089 XF BID BUGTRAQ OSVDB MILWoRM MISC
qsoft -- k-rate	Multiple cross-site scripting (XSS) vulnerabilities in Qsoft K-Rate Premium allow remote attackers to inject arbitrary web script or HTML via the blog, possibly the (1) Title and (2) Text fields; (3) the gallery, possibly the Description field in Your Pictures; (4) the forum, possibly the Your Message field when posting a new thread; or (5) the vote parameter in a view action to index.php. NOTE: some of these details are obtained from third party information.	2009-08-27	4.3	CVE-2008-7098 MILWoRM SECUNIA OSVDB OSVDB OSVDB

radvision -- scopia	Cross-site scripting (XSS) vulnerability in entry/index.jsp in Radvision Scopia 5.7, and possibly other versions before SD 7.0.100, allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2009-08-25	4.3	CVE-2009-2965 BUGTRAQ
sophos -- puremessage_for_microsoft_exchange	Sophos PureMessage Scanner service (PMScanner.exe) in PureMessage for Microsoft Exchange 3.0 before 3.0.2 allows remote attackers to cause a denial of service (message queue delay and incomplete spam rule update) via a crafted (1) RTF or (2) PDF file.	2009-08-27	5.0	CVE-2008-7104 CONFIRM
sophos -- puremessage_for_microsoft_exchange	Sophos PureMessage for Microsoft Exchange 3.0 before 3.0.2 allows remote attackers to cause a denial of service (EdgeTransport.exe termination) via a TNEF-encoded message with a crafted rich text body that is not properly handled during conversion to plain text. NOTE: this might be related to CVE-2008-7104.	2009-08-27	5.0	CVE-2008-7105 CONFIRM
sophos -- puremessage_for_microsoft_exchange	The installation of Sophos PureMessage for Microsoft Exchange 3.0 before 3.0.2, when both anti-virus and anti-spam are supported, does not create or launch the associated scan engines when the system is under heavy load, which has unspecified impact, probably remote bypass of scanner protection or a denial of service (message loss or delay).	2009-08-27	5.0	CVE-2008-7106 CONFIRM
squirrelmail -- squirrelmail	Multiple cross-site request forgery (CSRF) vulnerabilities in SquirrelMail 1.4.19 and earlier allow remote attackers to hijack the authentication of unspecified victims via features such as send message and change preferences, related to (1) functions/mailbox_display.php, (2) src/addrbook_search_html.php, (3) src/addressbook.php, (4) src/compose.php, (5) src/folders.php, (6) src/folders_create.php, (7) src/folders_delete.php, (8) src/folders_rename_do.php, (9) src/folders_rename_getname.php, (10) src/folders_subscribe.php, (11) src/move_messages.php, (12) src/options.php, (13) src/options_highlight.php, (14) src/options_identities.php, (15) src/options_order.php, (16) src/search.php, and (17) src/vcard.php.	2009-08-25	6.8	CVE-2009-2964 CONFIRM VUPEN CONFIRM CONFIRM CONFIRM
unica -- affinium_campaign	Multiple cross-site scripting (XSS) vulnerabilities in Unica Affinium Campaign 7.2.1.0.55 allow remote attackers to inject arbitrary web script or HTML via a Javascript event in the (1) url, (2) PageName, and (3) title parameters in a CustomBookMarkLink action to Campaign/Campaign; (4) a Javascript event in the displayIcon parameter to Campaign/updateOfferTemplateSubmit.do (aka the templates web page); (5) crafted input to Campaign/CampaignListener (aka the listener server), which is not properly handled when displaying the status log; and (6) id parameter to Campaign/campaignDetails.do, (7) id parameter to Campaign/offerDetails.do, (8) function parameter to Campaign/Campaign, (9) sessionID parameter to Campaign/runAllFlowchart.do, (10) id parameter in an edit action to Campaign/updateOfferTemplatePage.do, (11)	2009-08-26	4.3	CVE-2008-7092 XF XF XF BID MISC MISC MISC MISC OSVDB OSVDB OSVDB OSVDB OSVDB OSVDB OSVDB OSVDB

	Frame parameter in a LoadFrame action to Campaign/Campaign, (12) affiniumUserName parameter to manager/jsp/test.jsp, (13) affiniumUserName parameter to Campaign/main.do, and possibly other vectors.			OSVDB OSVDB SECUNIA
unica -- affinium_campaign	Multiple directory traversal vulnerabilities in Unica Affinium Campaign 7.2.1.0.55 allow remote attackers to (1) create arbitrary directories or files via a .. (dot dot) in the folder name in the new folder functionality or (2) list arbitrary files via a crafted request to Campaign/CampaignListener.	2009-08-26	6.8	CVE-2008-7093 XF XF BID MISC MISC OSVDB OSVDB SECUNIA
unica -- affinium_campaign	Campaign/CampaignListener in the listener server in Unica Affinium Campaign 7.2.1.0.55 allows remote attackers to cause a denial of service (server crash) via a crafted length field that triggers (1) connection exhaustion or (2) memory allocation failure.	2009-08-26	5.0	CVE-2008-7094 XF BID MISC OSVDB SECUNIA
visualshapers -- ezcontents	Multiple directory traversal vulnerabilities in ezContents 2.0.3 allow remote attackers to include and execute arbitrary local files via the (1) gsLanguage and (2) language_home parameters to modules/diary/showdiary.php; (3) admin_home, (4) gsLanguage, and (5) language_home parameters to modules/diary/showdiarydetail.php; (6) gsLanguage and (7) language_home parameters to modules/diary/submit_diary.php; (8) admin_home parameter to modules/news/news_summary.php; (9) nLink, (10) gsLanguage, and (11) language_home parameters to modules/news/inlinenews.php; and possibly other unspecified vectors in (12) diary/showeventlist.php, (13) gallery/showgallery.php, (14) reviews/showreviews.php, (15) gallery/showgallerydetails.php, (16) reviews/showreviewsdetails.php, (17) news/shownewsdetails.php, (18) gallery/submit_gallery.php, (19) guestbook/submit_guestbook.php, (20) reviews/submit_reviews.php, (21) news/submit_news.php, (22) diary/inlineeventlist.php, and (23) news/archivednews_summary.php in modules/, related to the lack of directory traversal protection in modules/moduleSec.php.	2009-08-24	5.1	CVE-2008-7054 XF BID BUGTRAQ OSVDB OSVDB OSVDB OSVDB OSVDB MILWoRM SECUNIA
visualshapers -- ezcontents	module.php in ezContents 2.0.3 allows remote attackers to bypass the directory traversal protection mechanism to include and execute arbitrary local files via "....//%" (doubled dot dot slash) sequences in the link parameter, which is not properly filtered using the str_replace function.	2009-08-24	5.1	CVE-2008-7055 XF BID BUGTRAQ MILWoRM SECUNIA
webdav -- neon	neon before 0.28.6, when expat is used, does not properly detect recursion during entity expansion, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML	2009-08-21	4.3	CVE-2009-2473 VITDENT

	document containing a large number of nested entity references, a similar issue to CVE-2003-1564.			VUPEN
webdav -- neon webv dav -- neon	neon before 0.28.6, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-08-21	6.8	CVE-2009-2474 VUPEN
webidsupport -- webid	eledicss.php in WeBid auction script 0.5.4 allows remote attackers to modify arbitrary cascading style sheets (CSS) files via a certain request with the file parameter set to style.css. NOTE: this can probably be leveraged for cross-site scripting (XSS) attacks.	2009-08-28	5.0	CVE-2008-7117 XF BID MILWoRM
webidsupport -- webid	WeBid auction script 0.5.4 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain SQL query logs via a direct request for logs/cron.log.	2009-08-28	5.0	CVE-2008-7118 XF BID MILWoRM

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- cs-mars	The Cisco Security Monitoring, Analysis and Response System (CS-MARS) 6.0.4 and earlier stores cleartext passwords in log/sysbacktrace.## files within error-logs.tar.gz archives, which allows context-dependent attackers to obtain sensitive information by reading these files.	2009-08-27	3.3	CVE-2009-2977 VUPEN BID BUGTRAQ BUGTRAQ CONFIRM

[Back to top](#)

Last updated August 31, 2009

 Print This Document